Penetration Tests in the Military Data Network Environment

Radek Beran

VÚ 3255, Dobrovského 6, Olomouc, 77111, Czech Republic
radek.beran@army.cz

Abstract. Security risks and threats targeted at information and information technology are each year more severe. A significant contribution to this is the fact that modern technologies increasingly penetrate our private and professional life. The sense of isolation of the global military data network from the outer dangerous world of the internet can create a false feeling of security. Both in users and in administrators of all information systems that use global data network as the transmission medium. This contribution would like to outline options for the use of internal penetration tests in routine operation of military data networks. It mainly explores the possibilities of tools offered for system testing on the Microsoft Windows platform..

1 Introduction

The environment of the global data network of the Armed Forces of the Czech Republic is very heterogeneous and is used for data transfer by all operated information systems, voice systems and independently connected devices. For passive monitoring of network traffic and its anomalies there is a determined group called Computer Incident Response Capability (CIRC), which for its monitoring and evaluation uses distributed probes that capture and evaluate network traffic based on the known and from the internet resources updated templates. In this there can be observed a certain positive development, but in practice we find that new technology often brings new problems, or does not solve the known problems, and that it cannot be considered in complete isolation.
Weaknesses previously negligible can become more severe due to changes in user behaviour, the number of users, the amount of knowledge and, in general, the way in which the technology is used and how much depends on it. We also often encounter cases where technology offers a possibility of protection, but in practice it is not used, e.g. from ignorance or simply because of convenience.

2 Definitions of Terms and Classification of the Topic

A penetration test is, in short, a planned use of existing attack techniques and tactics used for intrusions into the corporate IT infrastructure to detect weaknesses in the security of the infrastructure. Configuration errors and other security gaps in protection are used and detected. Penetration tests provide current information on the status of systems and practical verification of the set security policy. System approach to corporate security (see e.g. OSSTMM) requires a sophisticated mix of used tests and their implementation at periodic intervals, while it is advisable from time to time to change the supply company to avoid long-term one-sided results.
Penetration testing began in the early 1990s. Due to the action of one of the first computer worms a large number of users realized the vulnerability of existing computer systems, the price of data stored in those systems, their weaknesses and the importance of security. Since that moment tools enabling to check the IT systems settings began to appear. It was mostly a number of diverse scripts that were checking local configurations. One of the first was for example SATAN. Nowadays, there is a large number of such tools and their range corresponds with increasing potential threats.

3 The Specifics of Military Environment

Currently the MoD runs in Internal Military Data Network Environment the following major information systems:

- Staff Information System (Štábní informační systém - ŠIS)
- Logistics Information System (Informační systém logistiky – ISL)
- Service and Personnel Information System (Informační systém o službě a personálu – ISSP)
- Mobilization Preparations Information System (Informační systém mobilizačních příprav)
- Military Police Information System (Informační systém Vojenské policie)
- Military Health Information System (Informační systém vojenského zdravotnictví – ZDRAVIS)

All the above mentioned information systems are departmental. The MoD does not operate any information system of public administration. For several years, the resort has been preparing a cross-sectional information system that should replace the still-functioning information systems.
The above mentioned information systems support management of the activities of the Ministry of Defence, including administrative and staff activities, management of departmental resources (human, financial and material), further supporting the work of the military services and command and control operations.
As seen in the preceding summary, there are quite a lot of information systems. However, a penetration test has not been run in any of them so far.

4 The Process of Penetration Test

The first step in the penetration testing design is to determine the correct type of test and the extent and manner of testing. Penetration tests can be focused on infrastructure or application environment. Each of these tests is focused on different types of vulnerabilities, therefore it requires a different approach, tools and evaluation. In the concept draft I will abide by following processes and individual phases of the testing itself. I examined the hypothesis that the optimal method of application penetration testing in the military environment is a test of the internal network, and in terms of accuracy and speed of implementation of each process, I will assume full knowledge of the environment and system, i.e. white box non-destructive tests.

Fig. 1. The Process of Penetration Test

4.1 Preparation before Performance

At this stage it is necessary to arrange an agreement with system administrators and operators and inform all interested and responsible parties. Then suggest a testing schedule and the resulting planned shutdown of the system. Lastly, assemble a team of implementers and a support team and accurately allocate responsibility for each subsequent phase. Proactive testing could, in certain cases, be classified as a criminal offense and assessed according to the Czech Criminal Code (Act No.40/2009 Sb., Part Two, special part, § 230 Unauthorized access to computer system and data carrier).

4.2 Survey – The Objective and Scope of Penetration Test

In the first step, the tester tries to get as much information about the objective. They can obtain it actively or passively. During the active research the tester uses various tools to search the network to, for example, ascertain the extent of IP addresses, name servers and contact names. Passive survey indicates browsing through other freely available materials about the test object, such as intranet sites and other sites, from which they can learn useful facts, such as what types of software and technology are used.
The tester should receive all such information from the cooperative team. Despite this, it is necessary to not underestimate this stage and perform a careful survey. In the system there may be no longer used, forgotten assets that were until recently a part of the system and misuse of their weaknesses could lead to breaking into the system.
When setting objectives and scope of penetration testing, it is recommended to use a systemic approach. With its help there are at first formulated questions, to which are subsequently sought answers. On the basis of these answers it will be easier to specify the objectives of individual tests and to identify means and ways to find answers to the questions, which will in the end create the report on the overall level of security.

4.3 Scanning – Data Collection

In this part the tester is trying to find mistakes in the target network that will enable them to break into the system. They scan ports and determine what services run on them and compare them to lists of known network errors. Using the NetBIOS protocol they try to make a list of network drives and find unpatched operating system parts. The result of the scan should therefore be a list of systems that they might be able to gain control over due to security flaws.

4.3.1 Checking infrastructure security at the physical level

Preventing unwanted access and adverse action on the part of users and trespassers is the main objective of securing the infrastructure. These are mainly:

- Illegal and unwanted settings and changes of hardware
- Interference with the equipment, leading to a partial or complete loss of function
- Theft of the device or its important technological part

Necessary locking of all the key elements of the infrastructure into a room limited with access for selected people only is just one of the levels of hardware infrastructure security. To the hardware infrastructure belongs also the equipment normally available during working hours in the hallways, such as fax machines, printers, copiers, shredders and open switch ports. Checking the available devices and attempting to intervene in the setting may be a short and simple test. If it is successful, and therefore any user can intervene in the structure and settings, it found a weak point and the device can become a target of attack.

4.3.2 Checking infrastructure software security

These include, for example, setting an access password to BIOS of a desktop computer and preventing booting from portable media. This does not include, however, only endpoints. You should also configure the password to printers and other devices freely available. Usually the installation of these devices is hectic and if everything is working properly then there is no real reason to change the default password given by the manufacturer. Thus another weak spot is created.

4.4 Gaining Access – Exploitation

Based on information obtained in the previous processes, the tester creates a breach plan. According to the list of ulnerabilities, which was gained during scanning and survey, the tester can now target the weak points and through them gain access to the system. The tester uses a variety of exploits on the errors that were found. The aim is to obtain the highest possible user rights on the compromised system, preferably the domain administrator privileges. Ethical hacker also acquires evidence during hacking that is a part of the final report and recommendations for improvement for the system operator.

4.5 Evaluation – the Final Report

During the course of preceding processes, detailed data on the characteristics of the system and all action taken must be gathered and collected. A summary of this information is elaborated in the final report of the progress and results of the testing. For each identified deficiency or vulnerability there should be a commentary suggesting possible solutions. The final report is then forwarded in a pre-agreed manner to the contracting authority, usually processed in two viewpoints – general managerial and detailed administrator.

4.6 Remedy or Acceptance of Vulnerabilities

Without the implementation of the relevant steps that will lead to an improvement of the system, testing would be useless. According to the obtained results the priorities will be determined – which problems have the solution priority, which can be remedied later or there will be a decision to accept some of the vulnerabilities. All the steps must be documented and will serve as the basis for the repeat test.

5 Testing the Software Tools

An important prerequisite for any further testing of vulnerability are automatic scanners. Due to the occupation of Internal Global Data Network environment by many information systems and the threat of collapse of one of them during analyzing the ability of individual scanning solutions, there was a virtual environment with a separate network interface installed for the testing of the scanners. Through analyzing the military network environment, I came to the conclusion, that the optimal base for penetration tests will be internal test. Also the form of white-box is according to the analysis the most appropriate, as the managers, operators and security officers know in detail the configuration of individual assets and support systems. These data they transmit to the realization penetration team for detailed familiarization and preparation of the test itself.

5.1 Compilation for Penetration Testing

A large number of various, mostly software tools for penetration testing can be found on the internet. The effort expanded on gathering them all to a whole complex and then categorizing them according to their purpose would be very time-consuming and mostly unnecessary. This work has been done for us by enthusiasts and those interested in computer security, and also by hackers and security administrators. They compiled so-called distributions, largely based on one of the versions of the Linux operating system. Among the best-known, most widely used and also the highest rated belong the following penetration distributions.

5.1.1 Pentoo

Pentoo is a distribution based on Gentoo Linux and is aimed on testing security of IT systems by collecting tools for following areas:

- Analyzers – arpwatch, jxplorer, socat, netdiscover, ngrep, ntop, thcrut, wireshark
- Bluetooth scanners
- Password crackers – cewl, hydra, John The Ripper, medusa, ophcrack
- Databases – mssqlscan, sqlninja, sqlmap
- Exploits – beef, w3af, Metasploit Security Framework, armitage
- Forensic analysis – galleta, hivex, origami tools, rdd
- Forgery – gspoof, macchanger, nemesis, netwib/netwag, rain
- Man-in-the-middle attacks – dsniff, ettercap, brctl
- Scanners – nikto, wapiti, nmap, hunt, arachni, skipfish
- Wireless networks – aircrack-ng, airsnort, kismet,wepattack, wifite

5.1.2 Kali Linux

Kali Linux is a Linux distribution based on Debian, designed for digital forensic analysis and penetration tests. It presents a modified original distribution BackTrack, it is fully compatible with the Debian development platform, to which also corresponds the full synchronization with the respective Debian update repositories. The distribution is intended for the use in security testing in organizations environment. Kali Linux is currently managed and updated and funded by a company called Offensive Security. The company offers penetration tests

as a service and also provides training and coaching. In addition, the company manages a database of exploits and a free internet course called Metasploit Unleashed.

6 Tools for Automatic Scanning – Collecting Data

To get information on the corporate network and find weaknesses and potential targets for attack it is necessary to gather all the available information. How to get it and which tools, from which this information may be obtained, to use, I will present in the following text.

6.1 GFI LANguard

The one-in-all solution from the GFI company called GFI Languard serves for scanning and network audit, open ports detection, evaluation and correction of security vulnerabilities, management of operating systems security patches, third party applications and solutions for several other areas.

6.2 Nessus

I mention Nessus Scanner intentionally, because during the analysis of military data network environment I found that this scanner had already been purchased and is on demand used by CIRC for vulnerability testing. Its installation and activation, for example into the environment of a virtual machine Oracle VM VirtualBox with Kali Linux penetration distribution on a portable computer, will enable flexible use in different network segments and information systems. Nessus itself in a variant for the Linux operating system is offered for Kali Linux.
It is a very well known and popular vulnerability scanner, first published in 1998 by Renaud Deraison and currently managed by Tenable Network Security. There are several paid versions and a free version Nessus Home available for home and non-commercial use. There is also a version released under GPL, separated from Nessus 2 under the name OpenVAS.
The core of Nessus is based on plugins, which makes it possible to identify a large number of vulnerabilities. Currently (2015), Nessus uses more than 60 000 of them. New plugins are, according to published or found vulnerabilities, created within 24 hours and published on the website of the producer.

7 Metasploit Framework

The world's most popular and most widely used software for professional penetration testing. Currently it is owned and developed by a company called Rapid7, for non-commercial use there is a Metasploit Community Edition available. Framework is integrated with Nexpose vulnerability scanner from the same company. Its great advantage is that it really safely simulates real attacks, monitors safety measures and shows their weaknesses and also audits web applications. Versions are available for Windows and Linux and it includes an open API for further development.
In the Kali Linux environment, Metasploit Framework is already installed, but according to the set policy of services it stands that what is not needed, is not running, and it is up to the user to get the needed services launched and set.

Conclusion

In my opinion and experience, security testing of information systems in an isolated corporate network is a slightly neglected matter. Security personnel set rules and monitor log files, certainly to the best of their knowledge and belief, obviously in cooperation with the administration and operation of these systems, but the impact of the changes that appear throughout the life cycle of the information process is not usually examined. So by the emergence of new functionalities, there can occur, even if unintentionally, an emergence of new vulnerabilities. Therefore, it is necessary not only to periodically assess vulnerabilities and to keep an overview, but also to test them.

Literature

[1] BARCELÓ, Marta a Pete HERZOG. OSSTMM 3: The Open Source Security Testing Methodology Manual. In: BARCELÓ,. *OSSTMM 3: The Open Source Security Testing Methodology Manual* [online]. 2010 [cit. 2015-02-25]. Dostupné z: http://www.isecom.org/ mirror/OSSTMM.3.pdf

[2] ALLEN, Lee, Tedi HERIYANTO a Shakeel ALI. *Kali linux: assuring security by penetration testing*. Second Edition. S.l.: Packt Publishing Limited, 2014. ISBN 978-184-9519-489.

[3] BROAD, James a Andrew BINDNER. *Hacking with Kali: practical penetration testing techniques*. First edition. 225 Wyman Street, Waltham, MA 02451, USA: Syngress, 2014, ix, 227 pages. ISBN 978-012-4077-492.

[4] ENGEBRETSON, Pat a James BROAD. *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Waltham, MA: Syngress, 2011, xvii, 159 p. ISBN 15-974-9655-3.